(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－350678
（P2001－350678A）
(43)公開日　平成13年12月21日(2001.12.21)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　13/00	３５１	Ｇ０６Ｆ　13/00	３５１Ｚ	５Ｂ０８９
Ｈ０４Ｌ　12/22		Ｈ０４Ｌ　11/26		５Ｋ０３０

審査請求　未請求　請求項の数13　ＯＬ　（全 19 頁）

(21)出願番号　特願2000－170727(P2000－170727)

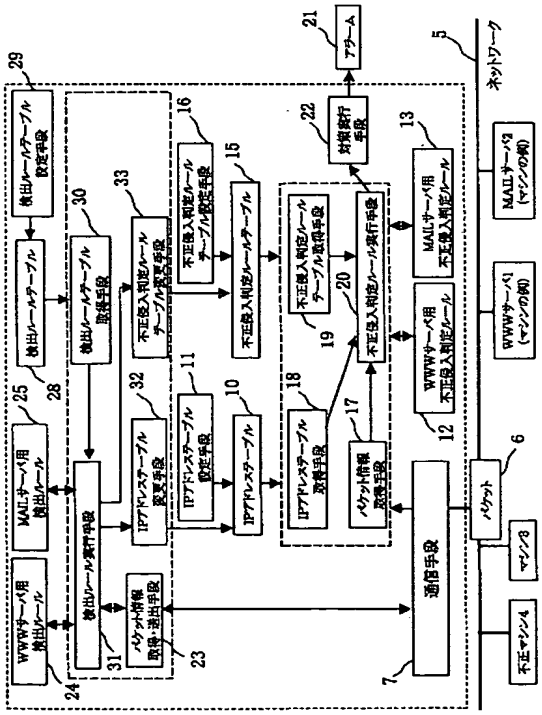
(22)出願日　平成12年６月７日(2000.6.7)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(72)発明者　小林　信博
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(74)代理人　100099461
弁理士　溝井　章司　（外２名）

Ｆターム(参考)　5B089 GA11 GA21 GB02 KA17 KB13
5K030 GA15 GA17 HA08 HB28

(54)【発明の名称】　不正侵入検知システム

(57)【要約】
【課題】　ＩＰアドレステーブルと不正侵入判定ルールテーブルを用いて、不正侵入判定を行なう不正侵入検知システムに係り、ＩＰアドレステーブルと不正侵入判定ルールテーブルの設定変更を自動的に行う不正侵入検知システムを提供することを課題とする。
【解決手段】　検出ルール実行手段３１の動作結果に基づいて、ＩＰアドレステーブル変更手段３２が、ＩＰアドレステーブル１０を変更し、不正侵入判定ルールテーブル変更手段３３が、不正侵入判定ルールテーブル１５を変更し、これらのテーブルを用いて、不正侵入判定ルール実行手段２０は、不正侵入の判定を行なう。



1

【特許請求の範囲】

【請求項１】　ネットワークを介してマシンに接続し、マシンに対する不正侵入を検知する不正侵入検知システムであって、以下の要素を有することを特徴とする不正侵入検知システム（１）ネットワークに接続するマシンの識別情報と、マシンのＩＰアドレスとを対応つけて記憶するＩＰアドレステーブル、（２）ネットワークに接続するマシンの識別情報と、マシンに対する不正侵入を判定する不正侵入判定ルールの識別情報とを対応付けて記憶する不正侵入判定ルールテーブル、（３）ネットワークを介してパケットの送受信を行なう通信手段、

（４）通信手段からパケットを取得し、取得したパケットに含まれるＩＰアドレスを取り出すパケット情報取得手段、（５）ＩＰアドレステーブルから、パケット情報取得手段により取り出したＩＰアドレスと一致するＩＰアドレスに対応するマシンの識別情報を選択し、

不正侵入判定ルールテーブルから、選択したマシンの識別情報と一致する識別情報に対応する不正侵入判定ルールの識別情報を選択し、

選択した識別情報で識別される不正侵入判定ルールに従って、不正侵入を判定する不正侵入判定ルール実行手段、（６）通信手段からパケットを取得し、

取得したパケットに含まれるＩＰアドレスを取り出し、

取り出したＩＰアドレスで特定されるマシンに対して接続し、

接続したマシン上で動作しているサーバの種類を取得し、

取得したサーバの種類に適した不正侵入判定ルールを選択し、

接続したマシンの識別情報を生成する検出ルール実行手段、

（７）検出ルール実行手段により生成したマシンの識別情報と、取り出したＩＰアドレスとを対応つけて、ＩＰアドレステーブルに記憶させるＩＰアドレステーブル変更手段、（８）検出ルール実行手段により生成したマシンの識別情報と、選択した不正侵入判定ルールの識別情報とを対応付けて、不正侵入判定ルールテーブルに記憶させる不正侵入判定ルールテーブル変更手段。

【請求項２】　不正侵入検知システムは、更に、サーバの種類と、そのサーバの種類に適した不正侵入判定ルールの識別情報とを対応つけて記憶する検出ルールテーブルを有し、

検出ルール実行手段は、検出ルールテーブルで、サーバの種類に対応つけられる不正侵入判定ルールの識別情報を出力することを特徴とする請求項１記載の不正侵入検知システム。

【請求項３】　不正侵入検知システムは、更に、ＩＰアドレステーブルに、検出ルール実行手段により取り出したＩＰアドレスと一致するＩＰアドレスが記憶されているかを検査するＩＰアドレス設定済検査手段を有し、

2

ＩＰアドレステーブル変更手段は、ＩＰアドレス設定済検査手段により、一致するＩＰアドレスが記憶されていないと判断した場合に、検出ルール実行手段により生成したマシンの識別情報と、取り出したＩＰアドレスとを対応つけて、ＩＰアドレステーブルに記憶させることを特徴とする請求項１記載の不正侵入検知システム。

【請求項４】　不正侵入検知システムは、更に、不正侵入判定ルールテーブルに、検出ルール実行手段により選択した不正侵入判定ルールの識別情報と一致する識別情報が記憶されているかを検査する不正侵入判定ルール設定済検査手段を有し、

不正侵入判定ルールテーブル変更手段は、不正侵入判定ルール設定済検査手段により、一致する不正侵入判定ルールの識別情報が記憶されていないと判断した場合に、検出ルール実行手段により生成したマシンの識別情報と、選択した不正侵入判定ルールの識別情報とを対応付けて、不正侵入判定ルールテーブルに記憶させることを特徴とする請求項１記載の不正侵入検知システム。

【請求項５】　不正侵入検知システムは、更に、ＩＰアドレステーブルから、マシンの識別情報と、マシンのＩＰアドレスとを取得するＩＰアドレステーブル再取得手段と、

不正侵入判定ルールテーブルから、ＩＰアドレステーブル再取得手段により取得したマシンの識別情報と一致する識別情報に対応する不正侵入判定ルールの識別情報を取得する不正侵入判定ルールテーブル再取得手段と、

検出ルール実行手段に、ＩＰアドレステーブル再取得手段により取得したＩＰアドレスで特定されるマシンに接続させ、接続したマシン上で動作しているサーバの種類を取得させる検出ルール再実行手段とを有し、

不正侵入判定ルールテーブル変更手段は、不正侵入判定ルールテーブル再取得手段により取得した不正侵入判定ルールの識別情報により識別される不正侵入識別ルールが適するサーバの種類と、ルール実行手段により取得したサーバの種類とが一致しない場合に、

不正侵入判定ルールテーブルから、不正侵入判定ルールテーブル再取得手段により取得した不正侵入判定ルールの識別情報を削除することを特徴とする請求項１記載の不正侵入検知システム。

【請求項６】　不正侵入検知システムは、更に、ＩＰアドレステーブルから、マシンの識別情報と、マシンのＩＰアドレスとを取得するＩＰアドレステーブル再取得手段と、

検出ルール実行手段に、ＩＰアドレステーブル再取得手段により取得したＩＰアドレスで特定されるマシンに接続させる検出ルール再実行手段とを有し、

ＩＰアドレステーブル変更手段は、検出ルール実行手段による接続ができない場合に、ＩＰアドレステーブルから、ＩＰアドレステーブル再取得手段により取得したマシンの識別情報と、マシンのＩＰアドレスとを削除し、

不正侵入判定ルールテーブル変更手段は、ＩＰアドレステーブル再取得手段により取得したマシンの識別情報と、その識別情報に対応する不正侵入判定ルールの識別情報とを削除することを特徴とする請求項１記載の不正侵入検知システム。

【請求項７】　不正侵入検知システムは、更に、不正侵入判定ルール手段により不正侵入があったことを判定した場合に、対策としてアラームを出力する対策実行手段と、

対策実行手段により出力されたアラームを検知するアラーム検出手段と、

アラーム検出手段によりアラームを検出した場合に、検出ルール再実行手段を起動する再検出指定手段とを有することを特徴とする請求項５または６記載の不正侵入検知システム。

【請求項８】　不正侵入検知システムは、更に、検出ルールテーブルを暗号化する検出ルールテーブル暗号設定手段と、

暗号化した検出ルールテーブルを復号する検出ルールテーブル復号取得手段と、

ＩＰアドレステーブルを暗号化するＩＰアドレステーブル暗号設定手段と、

暗号化したＩＰアドレステーブルを復号するＩＰアドレステーブル復号取得手段と、

不正侵入判定ルールテーブルを暗号化する不正侵入判定ルールテーブル暗号設定手段と、

暗号化した不正侵入判定ルールテーブルを復号する不正侵入判定ルールテーブル復号取得手段とを有することを特徴とする請求項２記載の不正侵入検知システム。

【請求項９】　不正侵入検知システムは、更に、検出ルールテーブルと、ＩＰアドレステーブルと、不正侵入判定テーブルとの変更履歴を生成するテーブル変更保存手段と、

テーブル変更保存手段により生成した変更履歴を格納する履歴テーブルとを有することを特徴とする請求項１記載の不正侵入検知システム。

【請求項１０】　不正侵入検知システムは、更に、通信手段からパケットを取得して保存するパケット保存手段と、

パケット保存手段に保存したパケット出力するパケット再生手段とを有し、

検出ルール実行手段は、パケット再生手段により出力されるパケットを取得することを特徴とする請求項１記載の不正侵入検知システム。

【請求項１１】　不正侵入検知システムは、更に、パケット再生手段がパケットを出力するスケジュールを記憶する再生スケジュール記憶部と、

再生スケジュール記憶部に記憶するスケジュールに従って、パケット再生手段へパケットの出力を指示する指定日時パケット再生指示手段とを有することを特徴とする

請求項１０記載の不正侵入検知システム。

【請求項１２】　不正侵入検知システムは、更に、システムの負荷状況を取得する負荷取得手段と、

負荷取得手段により取得した負荷状況が、所定の負荷よりも小さいと判断した場合に、パケット再生手段へパケットの出力を指示する低負荷時パケット再生指示手段とを有することを特徴とする請求項１０記載の不正侵入検知システム。

【請求項１３】　不正侵入検知システムは、更に、パケット保存手段からパケットの流通量を取得するパケット流通量取得手段と、

パケット流通量取得手段により取得したパケットの流通量が、所定の流通量よりも少ないと判断した場合に、パケット再生手段へパケットの出力を指示する低ネットワーク負荷時パケット再生指示手段とを有することを特徴とする請求項１０記載の不正侵入検知システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、ネットワーク上を流れるパケットを入手して動作する不正侵入検知システムの設定方法に関する。

【０００２】

【従来の技術】図１７は、例えばコンピュータ・セキュリティ・シンポジウム’９９にて発表された「パケット監視によるネットワーク侵入検出システムの実装と評価」に代表されるような従来の侵入検知システムである。

【０００３】ネットワーク５は、ＷＷＷサーバ１、ＭＡＩＬサーバ２、正常マシン３、不正マシン４などを接続している。ネットワーク５上には、データ転送の為にパケット６が流れている。

【０００４】そのため、不正侵入検知システムは、通信手段７、ＩＰアドレステーブル１０、ＩＰアドレステーブル設定手段１１、ＷＷＷサーバ用不正侵入判定ルール１２、ＭＡＩＬサーバ用不正侵入判定ルール１３、不正侵入判定ルールテーブル１５、不正侵入判定ルールテーブル設定手段１６、パケット情報取得手段１７、ＩＰアドレステーブル取得手段１８、不正侵入判定ルールテーブル取得手段１９、不正侵入判定ルール実行手段２０、対策実行手段２２を備えている。

【０００５】通信手段７は、ネットワーク５とパケット６のやりとりを行う。

【０００６】ＩＰアドレステーブル１０は、マシン名８とＩＰアドレス９の関係をまとめたＩＰアドレスリストを記述している。尚、マシン名８は、ＷＷＷサーバ１、ＭＡＩＬサーバ２、正常マシン３や不正マシン４などを識別する。また、ＩＰアドレス９は、ＷＷＷサーバ１やＭＡＩＬサーバ２や正常マシン３や不正マシン４などが送受するパケット６の中に含まれるＩＰアドレスである。

【０００７】ＩＰアドレステーブル設定手段１１は、ＩＰアドレステーブル１０を設定する。

【０００８】WWWサーバ用不正侵入判定ルール１２は、パケット６の情報をもとにWWWサーバに対する不正侵入を判定するルールである。

【０００９】ＭＡＩＬサーバ用不正侵入判定ルール１３は、パケット６の情報をもとにＭＡＩＬサーバに対する不正侵入を判定するルールである。

【００１０】不正侵入判定ルールテーブル１５は、マシン名８と不正侵入判定ルール名１４の関係をまとめた不正侵入判定ルールリストを記述している。尚、不正侵入判定ルール名１４は、WWWサーバ用不正侵入判定ルール１２やＭＡＩＬサーバ用不正侵入判定ルール１３などを識別するルール名である。

【００１１】不正侵入判定ルールテーブル設定手段１６は、不正侵入判定ルールテーブル１５を設定する。

【００１２】パケット情報取得手段１７は、通信手段７からパケット６を取得する。

【００１３】ＩＰアドレステーブル取得手段１８は、ＩＰアドレステーブル１０からＩＰアドレスリストを取得する。

【００１４】不正侵入判定ルールテーブル取得手段１９は、不正侵入判定ルールテーブル１５から不正侵入判定ルールリストを取得する。

【００１５】不正侵入判定ルール実行手段２０は、ＩＰアドレスリストから、パケット６から取り出したＩＰアドレス９に対応するマシン名８を特定し、不正侵入判定ルールテーブルリストからそのマシン名８に対応する不正侵入判定ルールを特定し、その不正侵入判定ルールを実行する。

【００１６】対策実行手段２２は、不正侵入判定ルール実行手段２０の結果に応じて、アラーム出力などの制御を行なう。これにより、不正侵入判定ルール実行結果が不正侵入と判定されたときにアラームが出力する。

【００１７】このような従来の侵入検知システムにおいては、パケット情報取得手段１７により通信手段７から得られたパケット６を利用し、ＩＰアドレステーブル設定手段１１によってユーザーから設定されたＩＰアドレステーブル１０と、不正侵入判定ルールテーブル設定手段１６によってユーザーから設定された不正侵入判定ルールテーブル１５に基づき、不正侵入判定ルール実行手段２０が該当する不正侵入判定ルールを呼び出して侵入検知を行う。

【００１８】従来の侵入検知システムにおいては、ユーザーが手作業によりＩＰアドレステーブル１０と不正侵入判定ルールテーブル１５を設定していた為、煩雑であるという欠点があった。

【００１９】また、マシンが追加された場合にユーザが再設定しなくてはならないという欠点があった。

【００２０】また、マシン上で新たなサーバが実行されるようになった場合にユーザが再設定しなくてはならないという欠点があった。

【００２１】また、設定時にユーザが操作ミスを犯して意図しない設定のまま実行されるという問題もあった。

【００２２】

【発明が解決しようとする課題】本発明は、上記した従来技術の欠点を除くためになされたものであって、ＩＰアドレステーブルと不正侵入判定ルールテーブルの設定変更を自動的に行うものである。

【００２３】また、マシンが追加された場合に自動的にＩＰアドレステーブルを変更する。

【００２４】また、そのマシン上で稼働しているサーバを自動的に判定し、不正侵入判定ルールテーブルを変更する。

【００２５】また、マシン上で新たなサービスが稼働した場合に自動的に不正侵入判定ルールテーブルを変更する。

【００２６】

【課題を解決するための手段】この発明に係る不正侵入検知システムは、ネットワークを介してマシンに接続し、マシンに対する不正侵入を検知する不正侵入検知システムであって、以下の要素を有することを特徴とする。

（１）ネットワークに接続するマシンの識別情報と、マシンのＩＰアドレスとを対応つけて記憶するＩＰアドレステーブル、（２）ネットワークに接続するマシンの識別情報と、マシンに対する不正侵入を判定する不正侵入判定ルールの識別情報とを対応付けて記憶する不正侵入判定ルールテーブル、（３）ネットワークを介してパケットの送受信を行なう通信手段、（４）通信手段からパケットを取得し、取得したパケットに含まれるＩＰアドレスを取り出すパケット情報取得手段、（５）ＩＰアドレステーブルから、パケット情報取得手段により取り出したＩＰアドレスと一致するＩＰアドレスに対応するマシンの識別情報を選択し、不正侵入判定ルールテーブルから、選択したマシンの識別情報と一致する識別情報に対応する不正侵入判定ルールの識別情報を選択し、選択した識別情報で識別される不正侵入判定ルールに従って、不正侵入を判定する不正侵入判定ルール実行手段、（６）通信手段からパケットを取得し、取得したパケットに含まれるＩＰアドレスを取り出し、取り出したＩＰアドレスで特定されるマシンに対して接続し、接続したマシン上で動作しているサーバの種類を取得し、取得したサーバの種類に適した不正侵入判定ルールを選択し、接続したマシンの識別情報を生成する検出ルール実行手段、（７）検出ルール実行手段により生成したマシンの識別情報と、取り出したＩＰアドレスとを対応つけて、ＩＰアドレステーブルに記憶させるＩＰアドレステーブル変更手段、（８）検出ルール実行手段により生成したマシンの識別情報と、選択した不正侵入判定ルールの識

別情報とを対応付けて、不正侵入判定ルールテーブルに記憶させる不正侵入判定ルールテーブル変更手段。

【００２７】また、不正侵入検知システムは、更に、サーバの種類と、そのサーバの種類に適した不正侵入判定ルールの識別情報とを対応つけて記憶する検出ルールテーブルを有し、検出ルール実行手段は、検出ルールテーブルで、サーバの種類に対応つけられる不正侵入判定ルールの識別情報を出力することを特徴とする。

【００２８】また、不正侵入検知システムは、更に、ＩＰアドレステーブルに、検出ルール実行手段により取り出したＩＰアドレスと一致するＩＰアドレスが記憶されているかを検査するＩＰアドレス設定済検査手段を有し、ＩＰアドレステーブル変更手段は、ＩＰアドレス設定済検査手段により、一致するＩＰアドレスが記憶されていないと判断した場合に、検出ルール実行手段により生成したマシンの識別情報と、取り出したＩＰアドレスとを対応つけて、ＩＰアドレステーブルに記憶させることを特徴とする。

【００２９】また、不正侵入検知システムは、更に、不正侵入判定ルールテーブルに、検出ルール実行手段により選択した不正侵入判定ルールの識別情報と一致する識別情報が記憶されているかを検査する不正侵入判定ルール設定済検査手段を有し、不正侵入判定ルールテーブル変更手段は、不正侵入判定ルール設定済検査手段により、一致する不正侵入判定ルールの識別情報が記憶されていないと判断した場合に、検出ルール実行手段により生成したマシンの識別情報と、選択した不正侵入判定ルールの識別情報とを対応付けて、不正侵入判定ルールテーブルに記憶させることを特徴とする。

【００３０】また、不正侵入検知システムは、更に、ＩＰアドレステーブルから、マシンの識別情報と、マシンのＩＰアドレスとを取得するＩＰアドレステーブル再取得手段と、不正侵入判定ルールテーブルから、ＩＰアドレステーブル再取得手段により取得したマシンの識別情報と一致する識別情報に対応する不正侵入判定ルールの識別情報を取得する不正侵入判定ルールテーブル再取得手段と、検出ルール実行手段に、ＩＰアドレステーブル再取得手段により取得したＩＰアドレスで特定されるマシンに接続させ、接続したマシン上で動作しているサーバの種類を取得させる検出ルール再実行手段とを有し、不正侵入判定ルールテーブル変更手段は、不正侵入判定ルールテーブル再取得手段により取得した不正侵入判定ルールの識別情報により識別される不正侵入識別ルールが適するサーバの種類と、ルール実行手段により取得したサーバの種類とが一致しない場合に、不正侵入判定ルールテーブルから、不正侵入判定ルールテーブル再取得手段により取得した不正侵入判定ルールの識別情報を削除することを特徴とする。

【００３１】また、不正侵入検知システムは、更に、ＩＰアドレステーブルから、マシンの識別情報と、マシンのＩＰアドレスとを取得するＩＰアドレステーブル再取得手段と、検出ルール実行手段に、ＩＰアドレステーブル再取得手段により取得したＩＰアドレスで特定されるマシンに接続させる検出ルール再実行手段とを有し、ＩＰアドレステーブル変更手段は、検出ルール実行手段による接続ができない場合に、ＩＰアドレステーブルから、ＩＰアドレステーブル再取得手段により取得したマシンの識別情報と、マシンのＩＰアドレスとを削除し、不正侵入判定ルールテーブル変更手段は、ＩＰアドレステーブル再取得手段により取得したマシンの識別情報と、その識別情報に対応する不正侵入判定ルールの識別情報とを削除することを特徴とする。

【００３２】また、不正侵入検知システムは、更に、不正侵入判定ルール手段により不正侵入があったことを判定した場合に、対策としてアラームを出力する対策実行手段と、対策実行手段により出力されたアラームを検知するアラーム検出手段と、アラーム検出手段によりアラームを検出した場合に、検出ルール再実行手段を起動する再検出指定手段とを有することを特徴とする。

【００３３】また、不正侵入検知システムは、更に、検出ルールテーブルを暗号化する検出ルールテーブル暗号設定手段と、暗号化した検出ルールテーブルを復号する検出ルールテーブル復号取得手段と、ＩＰアドレステーブルを暗号化するＩＰアドレステーブル暗号設定手段と、暗号化したＩＰアドレステーブルを復号するＩＰアドレステーブル復号取得手段と、不正侵入判定ルールテーブルを暗号化する不正侵入判定ルールテーブル暗号設定手段と、暗号化した不正侵入判定ルールテーブルを復号する不正侵入判定ルールテーブル復号取得手段とを有することを特徴とする。

【００３４】また、不正侵入検知システムは、更に、検出ルールテーブルと、ＩＰアドレステーブルと、不正侵入判定テーブルとの変更履歴を生成するテーブル変更保存手段と、テーブル変更保存手段により生成した変更履歴を格納する履歴テーブルとを有することを特徴とする。

【００３５】また、不正侵入検知システムは、更に、通信手段からパケットを取得して保存するパケット保存手段と、パケット保存手段に保存したパケット出力するパケット再生手段とを有し、検出ルール実行手段は、パケット再生手段により出力されるパケットを取得することを特徴とする。

【００３６】また、不正侵入検知システムは、更に、パケット再生手段がパケットを出力するスケジュールを記憶する再生スケジュール記憶部と、再生スケジュール記憶部に記憶するスケジュールに従って、パケット再生手段へパケットの出力を指示する指定日時パケット再生指示手段とを有することを特徴とする。

【００３７】また、不正侵入検知システムは、更に、システムの負荷状況を取得する負荷取得手段と、負荷取得

手段により取得した負荷状況が、所定の負荷よりも小さいと判断した場合に、パケット再生手段へパケットの出力を指示する低負荷時パケット再生指示手段とを有することを特徴とする。

【００３８】また、不正侵入検知システムは、更に、パケット保存手段からパケットの流通量を取得するパケット流通量取得手段と、パケット流通量取得手段により取得したパケットの流通量が、所定の流通量よりも少ないと判断した場合に、パケット再生手段へパケットの出力を指示する低ネットワーク負荷時パケット再生指示手段とを有することを特徴とする。

【００３９】

【発明の実施の形態】実施の形態１．以下本発明を図面に示す実施例に基づいて説明する。図１は、実施の形態１における侵入検知システムを示す図である。ネットワーク５は、WWWサーバ１、ＭＡＩＬサーバ２、正常マシン３、不正マシン４などを接続している。ネットワーク５上には、データ転送の為にパケット６が流れている。

【００４０】そのため、不正侵入検知システムは、通信手段７、ＩＰアドレステーブル１０、ＩＰアドレステーブル設定手段１１、WWWサーバ用不正侵入判定ルール１２、ＭＡＩＬサーバ用不正侵入判定ルール１３、不正侵入判定ルールテーブル１５、不正侵入判定ルールテーブル設定手段１６、パケット情報取得手段１７、ＩＰアドレステーブル取得手段１８、不正侵入判定ルールテーブル取得手段１９、不正侵入判定ルール実行手段２０、対策実行手段２２、パケット情報取得・送出手段２３、WWWサーバ用検出ルール２４、ＭＡＩＬサーバ用検出ルール２５、検出ルールテーブル２８、検出ルールテーブル設定手段２９、検出ルールテーブル取得手段３０、検出ルール実行手段３１、ＩＰアドレステーブル変更手段３２、不正侵入判定ルールテーブル変更手段３３を備える。

【００４１】通信手段７は、ネットワーク５とパケット６のやりとりを行う。

【００４２】ＩＰアドレステーブル１０は、マシン名８とＩＰアドレス９の関係をまとめたＩＰアドレスリストを記述している。図２は、ＩＰアドレステーブルの構成を示す図である。尚、マシン名８は、WWWサーバ１、ＭＡＩＬサーバ２、正常マシン３や不正マシン４などを識別する。また、ＩＰアドレス９は、WWWサーバ１やＭＡＩＬサーバ２や正常マシン３や不正マシン４などが送受するパケット６の中に含まれるＩＰアドレスである。

【００４３】ＩＰアドレステーブル設定手段１１は、ＩＰアドレステーブル１０を設定する。

【００４４】WWWサーバ用不正侵入判定ルール１２は、パケット６の情報をもとにWWWサーバに対する不正侵入を判定するルールである。

【００４５】ＭＡＩＬサーバ用不正侵入判定ルール１３は、パケット６の情報をもとにＭＡＩＬサーバに対する不正侵入を判定するルールである。

【００４６】不正侵入判定ルールテーブル１５は、マシン名８と不正侵入判定ルール名１４の関係をまとめた不正侵入判定ルールリストを記述している。図３は、ルールテーブルの構成を示す図である。尚、不正侵入判定ルール名１４は、WWWサーバ用不正侵入判定ルール１２やＭＡＩＬサーバ用不正侵入判定ルール１３などを識別するルール名である。

【００４７】不正侵入判定ルールテーブル設定手段１６は、不正侵入判定ルールテーブル１５を設定する。

【００４８】パケット情報取得手段１７は、通信手段７からパケット６を取得する。

【００４９】ＩＰアドレステーブル取得手段１８は、ＩＰアドレステーブル１０からＩＰアドレスリストを取得する。

【００５０】不正侵入判定ルールテーブル取得手段１９は、不正侵入判定ルールテーブル１５から不正侵入判定ルールリストを取得する。

【００５１】不正侵入判定ルール実行手段２０は、ＩＰアドレスリストから、パケット６から取り出したＩＰアドレス９に対応するマシン名８を特定し、不正侵入判定ルールテーブルリストからそのマシン名８に対応する不正侵入判定ルールを特定し、その不正侵入判定ルールを実行する。

【００５２】対策実行手段２２は、不正侵入判定ルール実行手段２０の結果に応じて、アラーム出力などの制御を行なう。これにより、不正侵入判定ルール実行結果が不正侵入と判定されたときにアラーム２１が出力する。

【００５３】パケット情報取得・送出手段２３は、通信手段７からパケット６を取得または送出する。

【００５４】WWWサーバ用検出ルール２４は、パケット６の情報をもとにWWWサーバ１かどうかの検出を行うルールである。

【００５５】ＭＡＩＬサーバ用検出ルール２５は、パケット６の情報をもとにＭＡＩＬサーバ２かどうかの検出を行うルールである。

【００５６】検出ルールテーブル２８は、種類２６と検出ルール２７とルール名１４の関係をまとめた検出ルールリストを記述している。図４は、検出ルールリストの構成を示す図である。尚、種類２６は、マシンがWWWサーバ１かＭＡＩＬサーバ２かなどを識別する。

【００５７】検出ルールテーブル設定手段２９は、検出ルールテーブル２８を設定する。

【００５８】検出ルールテーブル取得手段３０は、検出ルールテーブル２８から検出ルールリストを取り出す。

【００５９】検出ルール実行手段３１は、パケット６と検出ルールリストから検出ルール２７を実行し、検出ルール２７からの要求に応じてパケット情報取得・送出手

段２３とパケット６のやりとりを行い、検出結果を得る。いずれかのサーバを検出するまで、検出ルールリストにあるすべての検出ルールを実行する。

【００６０】ＩＰアドレステーブル変更手段３２は、検出結果を元にＩＰアドレステーブル１０を変更する。

【００６１】不正侵入判定ルールテーブル変更手段３３は、検出結果を元に不正侵入判定ルールテーブル１５を変更する。

【００６２】次に、動作について説明する。ＩＰアドレステーブル設定手段１１により、予めユーザはWWWサーバ１やＭＡＩＬサーバ２や正常マシン３や不正マシン４などを識別するマシン名８とＩＰアドレス９の関係をまとめたＩＰアドレスリストを記述したＩＰアドレステーブル１０を設定しておくことができる。

【００６３】また、不正侵入判定ルールテーブル設定手段１６により、予めユーザはマシン名８とWWWサーバ用不正侵入判定ルール１２やＭＡＩＬサーバ用不正侵入判定ルール１３などを識別するルール名１４の関係をまとめたルールリストを記述した不正侵入判定ルールテーブル１５を設定しておくことができる。

【００６４】そして、ユーザは、検出ルールテーブル設定手段２９により、マシンがWWWサーバ１かＭＡＩＬサーバ２かなどを識別する為の種類２６と、WWWサーバ用検出ルール２４又はＭＡＩＬサーバ用検出ルール２５の検出ルール２７と、WWWサーバ用不正侵入判定ルール１２やＭＡＩＬサーバ用不正侵入判定ルール１３などを識別するルール名１４を検出ルールテーブル２８に設定しておく。

【００６５】不正侵入検知システムは、通信手段７によりそのネットワーク５上でデータをのせて流れるパケット６を入手する。

【００６６】次に、パケット情報取得・送出手段２３により、通信手段７からパケット６を取得する。

【００６７】次に、検出ルールテーブル取得手段３０により、検出ルールテーブル２８から検出ルールリストを全て取り出す。

【００６８】次に、検出ルール実行手段３１により、パケット６と検出ルールリストから検出ルール２７を実行し、検出ルール２７からの要求に応じてパケット情報取得・送出手段２３とパケット６のやりとりを行い、検出結果を得る。この際に、パケット６は、パケット情報取得・送出手段２３と通信手段７を介し、ネットワーク５を経由して対象となるマシンと通信される。

【００６９】図５は、WWWサーバ用検出ルールの処理の流れである。Ｓ５０１により、検出ルール実行手段３１から実行されたWWWサーバ用検出ルール２４の処理が開始される。

【００７０】Ｓ５０２により、パケット６の中のＩＰアドレスを取得する。

【００７１】Ｓ５０３により、パケット６の中のＩＰアドレスに対して、ＰＯＲＴ番号８０の接続要求を送り、検出ルール実行手段３１からパケット情報取得・送出手段２３を経て通信手段７により実際のパケット６をネットワーク５に送出する。尚、ＰＯＲＴ番号８０は、WWWサーバのポート番号である。但し、ポート番号を指定せずに、１から順に確認する方法も考えられる。

【００７２】Ｓ５０４により、接続結果を確認する。接続成功の場合は、Ｓ５０５を実行する。接続失敗の場合は、Ｓ５０９へ移る。

【００７３】Ｓ５０５により、同一のＩＰアドレス及びポート番号に対して改行コードを２個送出し、検出ルール実行手段３１からパケット情報取得・送出手段２３を経て通信手段７により実際のパケット６をネットワーク５に送出する。

【００７４】Ｓ５０６により、ネットワークから取得したパケットを通信手段ならびにパケット情報取得・送出手段、更に検出ルール実行手段を経由してリプライとして受信する。

【００７５】Ｓ５０７により、リプライの先頭文字が“ＨＴＴＰ／１．０”から始まっているかどうかを比較する。一致した場合は、Ｓ５０８を実行する。不一致の場合は、Ｓ５０９へ移る。

【００７６】Ｓ５０８により、相手がWWWサーバであると判定する。尚、ＨＴＴＰプロトコルにより、WWWサーバがこのように動作することが定義されている。また、“ＨＴＴＰ／１．１”から始まっている場合にも、同様に判定することができる。

【００７７】Ｓ５０９により、一連の処理を終了する。

【００７８】尚、ＭＡＩＬサーバの場合には、ＰＯＲＴ番号は、２５番となり、ＨＥＬＯｔｅｓｔのリプライの先頭文字が”２５０”から始まっていることにより判定することができる。

【００７９】検出結果、新しいＩＰアドレス９が発見され、更にサーバが検出された場合には、ＩＰアドレステーブル変更手段３２によりＩＰアドレス９と、新たに生成したマシン名８をＩＰアドレステーブル１０に追加する。また、不正侵入判定ルールテーブル変更手段３３により、マシン名８とルール名１４を不正侵入判定ルールテーブル１５に追加する。

【００８０】次に、パケット情報取得手段１７により、通信手段７からパケット６を取得する。この際、通信手段７は自らがネットワーク５に送信したパケット６は渡さずに破棄する。

【００８１】次に、ＩＰアドレステーブル取得手段１８により、ＩＰアドレステーブル１０からパケット６の中に含まれるＩＰアドレス９に対応するＩＰアドレスリストを取得する。

【００８２】次に、不正侵入判定ルールテーブル取得手段１９により、不正侵入判定ルールテーブル１５からＩＰアドレスリストに含まれるマシン名８に対応するルー

ルテーブルリストを取得する。

【００８３】次に、不正侵入判定ルール実行手段２０により、ルールテーブルリストからルール名１４を取得して実行する。実行結果が不正侵入と判定されたときは、対策実行手段２２によりアラーム２１を出力する。

【００８４】従って、自動的に更新されたＩＰアドレステーブル１０と不正侵入判定ルールテーブル１５を用いて侵入検知が実行されることとなる。

【００８５】実施の形態２．図６は、実施の形態２における侵入検知システムを示す図である。本実施の形態における侵入検知システムは、前述の侵入検知システムの構成に加えて、ＩＰアドレス設定済検査手段４３を備えている。

【００８６】ＩＰアドレス設定済検査手段４３は、検出ルール実行手段３１から与えられたＩＰアドレス９がＩＰアドレステーブル１０に既に設定されているかどうかを検査して結果を検出ルール実行手段３１に渡す。

【００８７】動作について説明する。検出ルール実行手段３１により検出結果を得る処理までは、実施の形態１における動作と同様である。

【００８８】検出結果、新しいＩＰが発見され、更にサーバが検出された場合には、ＩＰアドレス９を検出ルール実行手段３１からＩＰアドレス設定済検査手段４３に渡し、ＩＰアドレス設定済検査手段４３により、ＩＰアドレステーブル１０に既に設定されているかどうかを検査する。そして、検査結果を検出ルール実行手段３１に渡す。

【００８９】ＩＰアドレス９が未登録の場合は、ＩＰアドレステーブル変更手段３２により、ＩＰアドレス９と新たに生成したマシン名をＩＰアドレステーブル１０に追加する。また、不正侵入判定ルールテーブル変更手段３３により、マシン名とルール名を不正侵入判定ルールテーブル１５に追加する。

【００９０】これ以降の動作は、実施の形態１における動作と同様である。

【００９１】本実施の形態では、ＩＰアドレステーブル１０にＩＰアドレス９が重複して設定されることがないので、ＩＰアドレステーブル１０が最適な状態に保たれる。

【００９２】実施の形態３．図７は、実施の形態３における侵入検知システムを示す図である。本実施の形態における侵入検知システムは、前述の侵入検知システムの構成に加えて、不正侵入判定ルール設定済検査手段４４を備えている。

【００９３】不正侵入判定ルール設定済検査手段４４は、検出ルール実行手段３１から与えられたマシン名８とルール名１４のペアであるルールリストが不正侵入判定ルールテーブル１５に既に設定されているかどうかを検査して結果を検出ルール実行手段３１に渡す。

【００９４】動作について説明する。検出ルール実行手段３１により検出結果を得る処理までは、実施の形態１における動作と同様である。

【００９５】検出結果、新しいＩＰが発見され、更にサーバが検出された場合には、マシン名８とルール名１４を検出ルール実行手段３１から不正侵入判定ルール設定済検査手段４４に渡し、不正侵入判定ルール設定済検査手段４４により、不正侵入判定ルールテーブル１５に既に設定されているかどうかを検査する。そして、検査結果を検出ルール実行手段３１に渡す。

【００９６】ルールリストが未登録の場合は、ＩＰアドレステーブル変更手段３２により、ＩＰアドレス９と新たに生成したマシン名をＩＰアドレステーブル１０に追加する。また、不正侵入判定ルールテーブル変更手段３３によりマシン名とルール名を不正侵入判定ルールテーブル１５に追加する。

【００９７】これ以降の動作は、実施の形態１における動作と同様である。

【００９８】本実施の形態では、不正侵入判定ルールテーブル１５にマシン名８とルール名１４のペアであるルールリストが重複して設定されることがないので、不正侵入判定ルールテーブル１５が最適な状態に保たれる。

【００９９】実施の形態４．図８は、実施の形態４における侵入検知システムを示す図である。本実施の形態における侵入検知システムは、前述の侵入検知システムの構成に加えて、ＩＰアドレステーブル再取得手段４５、不正侵入判定ルールテーブル再取得手段４６、検出ルール再実行手段４７、再検出指定手段４８を備えている。

【０１００】ＩＰアドレステーブル再取得手段４５は、ＩＰアドレステーブル１０からＩＰアドレスリストを再取得する。

【０１０１】不正侵入判定ルールテーブル再取得手段４６は、不正侵入判定ルールテーブル１５からルールリストを再取得する。

【０１０２】検出ルール再実行手段４７は、ＩＰアドレステーブル再取得手段４５より与えられるＩＰアドレスリストと、不正侵入判定ルールテーブル再取得手段４６より与えられるルールリストと、検出ルールテーブル取得手段３０より得られる検出ルールリストを用いて、検出ルール実行手段３１に再実行させる。

【０１０３】再検出指定手段４８は、検出ルール再実行手段４７に実行を指示する。

【０１０４】動作について説明する。ユーザは、任意の時点で再検出指定手段４８により検出ルール再実行手段４７に実行を指示することができる。

【０１０５】ＩＰアドレステーブル再取得手段４５は、ＩＰアドレステーブル１０からＩＰアドレスリストを再取得し、不正侵入判定ルールテーブル再取得手段４６は、不正侵入判定ルールテーブル１５からルールリストを再取得し、更に、検出ルールテーブル取得手段３０は、検出ルールリストを取得する。

15

【０１０６】検出ルール再実行手段４７は、ルールリスト中のルール名１４に対応する検出ルールリスト中の検出ルール２７と、ルールリスト中のマシン名８に対応するＩＰアドレステーブル１０中のＩＰアドレス９を取得し、これを検出ルール実行手段３１に渡して再実行させる。

【０１０７】次に、検出ルール実行手段３１により、検出ルール２７を実行し、検出ルール２７からの要求に応じてパケット情報取得・送出手段２３とパケット６のやりとりを行い検出結果を得る。

【０１０８】この際にパケット６は、パケット情報取得・送出手段２３と通信手段７を介し、ネットワーク５を経由して対象となるマシンと通信される。

【０１０９】検出結果、サーバが検出されなかった場合には、不正侵入判定ルールテーブル変更手段３３によりマシン名８とルール名１４を不正侵入判定ルールテーブル１５から削除する。また、ＩＰアドレス９が検出されなかった場合には、ＩＰアドレステーブル変更手段３２によりＩＰアドレス９とマシン名８をＩＰアドレステーブル１０から削除し、不正侵入判定ルールテーブル変更手段３３によりマシン名８とルール名１４を不正侵入判定ルールテーブル１５から削除する。

【０１１０】次に、パケット情報取得手段１７により、通信手段７からパケット６を取得する。この際、通信手段７は自らがネットワーク５に送信したパケット６は渡さずに破棄する。

【０１１１】次に、ＩＰアドレステーブル取得手段１８により、ＩＰアドレステーブル１０からパケット６の中に含まれるＩＰアドレス９に対応するＩＰアドレスリストを取得する。

【０１１２】次に、不正侵入判定ルールテーブル取得手段１９により、不正侵入判定ルールテーブル１５からＩＰアドレスリストに含まれるマシン名８に対応するルールテーブルリストを取得する。

【０１１３】次に、不正侵入判定ルール実行手段２０によりルールテーブルリストからルール名１４を取得して実行する。実行結果が不正侵入と判定された時は対策実行手段２２によりアラーム２１を出力する。

【０１１４】従って、再検出の指定のみで自動的に更新されたＩＰアドレステーブル１０と不正侵入判定ルールテーブル１５を用いて侵入検知が実行されることとなる。

【０１１５】実施の形態５．図９は、実施の形態５における侵入検知システムを示す図である。本実施の形態における侵入検知システムは、前述の侵入検知システムの構成に加えて、再検出指定手段４８、アラーム検出手段４９を備えている。

【０１１６】アラーム検出手段４９は、アラーム２１の出力を検出して、再検出指定手段４８に再検出を指示する。

16

【０１１７】本実施の形態では、ユーザが再検出指定手段４８を操作して検出ルール再実行手段４７に再実行を指示するかわりに、アラーム検出手段４９によりアラーム２１の発生を検出し、再検出指定手段４８に再実行を自動的に指示する。

【０１１８】従って、何らかの異常が発生または設定の更新が必要と考えられる場合に、迅速に対応することが可能となる。

【０１１９】実施の形態６．図１０は、実施の形態６における侵入検知システムを示す図である。本実施の形態における侵入検知システムは、前述の侵入検知システムの構成に加えて、設定時パスワード入力手段５１、起動時パスワード入力手段５２、実行時パスワード保存手段５３、暗号済検出ルールテーブル５４、検出ルールテーブル暗号設定手段５５、検出ルールテーブル復号取得手段５６、暗号済ＩＰアドレステーブル５７、ＩＰアドレステーブル暗号設定手段５８、ＩＰアドレステーブル復号取得手段５９、ＩＰアドレステーブル暗号変更手段６０、暗号済不正侵入判定ルールテーブル６１、不正侵入判定ルールテーブル暗号設定手段６２、不正侵入判定ルールテーブル復号取得手段６３、不正侵入判定ルールテーブル暗号変更手段６４を備えている。

【０１２０】本実施の形態におけるパスワード５０は、管理者しか知り得ぬパスワードである。

【０１２１】設定時パスワード入力手段５１は、設定時にパスワード５０を入力する。

【０１２２】起動時パスワード入力手段５２は、起動時にパスワード５０を入力する。

【０１２３】実行時パスワード保存手段５３は、起動時パスワード入力手段５２により入力されたパスワード５０を実行時にのみ保存する。

【０１２４】暗号済検出ルールテーブル５４は、パスワード５０により暗号化された検出ルールリストを格納する。

【０１２５】検出ルールテーブル暗号設定手段５５は、パスワード５０により暗号化して暗号済検出ルールテーブル５４を設定する。

【０１２６】検出ルールテーブル復号取得手段５６は、暗号済検出ルールテーブル５４よりパスワード５０にて復号した検出ルールリストを取得する。

【０１２７】暗号済ＩＰアドレステーブル５７は、パスワード５０により暗号化されたＩＰアドレスリストを格納する。

【０１２８】ＩＰアドレステーブル暗号設定手段５８は、パスワード５０により暗号化して暗号済ＩＰアドレステーブル５７を設定する。

【０１２９】ＩＰアドレステーブル復号取得手段５９は、暗号済ＩＰアドレステーブル５７よりパスワード５０にて復号したＩＰアドレスリストを取得する。

【０１３０】ＩＰアドレステーブル暗号変更手段６０

は、パスワード５０により復号し再度暗号化して暗号済ＩＰアドレステーブル５７を変更する。

【０１３１】暗号済不正侵入判定ルールテーブル６１は、パスワード５０により暗号化されたルールリストを格納する。

【０１３２】不正侵入判定ルールテーブル暗号設定手段６２は、パスワード５０により暗号化して暗号済不正侵入判定ルールテーブル６１を設定する。

【０１３３】不正侵入判定ルールテーブル復号取得手段６３は、暗号済不正侵入判定ルールテーブル６１よりパスワード５０にて復号したルールリストを取得する。

【０１３４】不正侵入判定ルールテーブル暗号変更手段６４は、パスワード５０により復号し、再度暗号化して暗号済不正侵入判定ルールテーブル６１を変更する。

【０１３５】動作について説明する。システム起動時に、管理者は、管理者しか知り得ぬパスワード５０を、起動時パスワード入力手段５２により入力し、実行時パスワード保存手段５３により実行中のみ保存する。

【０１３６】暗号済検出ルールテーブル５４には、パスワード５０により暗号化された検出ルールリストが格納される。暗号済検出ルールテーブル５４を設定する場合には、検出ルールテーブル暗号設定手段５５によりパスワード５０にて暗号化する。暗号済検出ルールテーブル５４により検出ルールリストを取得する場合には、検出ルールテーブル復号取得手段５６によりパスワード５０にて復号する。

【０１３７】暗号済ＩＰアドレステーブル５７には、パスワード５０により暗号化されたＩＰアドレスリストが格納される。暗号済ＩＰアドレステーブル５７を設定する場合には、ＩＰアドレステーブル暗号設定手段５８によりパスワード５０にて暗号化する。暗号済ＩＰアドレステーブル５７よりＩＰアドレスリストを取得する場合には、ＩＰアドレステーブル復号取得手段５９によりパスワード５０にて復号する。暗号済ＩＰアドレステーブル５７を変更する場合には、ＩＰアドレステーブル暗号変更手段６０によりパスワード５０にて復号し再度暗号化する。

【０１３８】暗号済不正侵入判定ルールテーブル６１には、パスワード５０により暗号化されたルールリストが格納される。暗号済不正侵入判定ルールテーブル６１を設定する場合には、不正侵入判定ルールテーブル暗号設定手段６２によりパスワード５０にて暗号化する。暗号済不正侵入判定ルールテーブル６１よりルールリストを取得する場合には、不正侵入判定ルールテーブル復号取得手段６３によりパスワード５０にて復号する。暗号済不正侵入判定ルールテーブル６１を変更する場合には、不正侵入判定ルールテーブル暗号変更手段６４によりパスワード５０にて復号し再度暗号化する。

【０１３９】この他の動作は、実施の形態１と同様である。

【０１４０】従って、管理者と当侵入検知システム以外の者により、設定情報が改ざんされることを防止できる。

【０１４１】実施の形態７．図１１は、実施の形態７における侵入検知システムを示す図である。本実施の形態における侵入検知システムは、前述の侵入検知システムの構成に加えて、検出ルールテーブル２８及びＩＰアドレステーブル１０及び検出ルールテーブル２８の変更履歴を格納する履歴テーブル６５と、検出ルールテーブル２８及びＩＰアドレステーブル１０及び検出ルールテーブル２８の変更履歴を履歴テーブル６５に格納するテーブル変更保存手段６６を備えている。

【０１４２】また、図１２は、この発明における履歴テーブルの構成の一例である。

【０１４３】本実施の形態では、検出ルールテーブル設定手段により、検出ルールテーブルを設定する際の履歴をテーブル変更保存手段により履歴テーブルに保存する。不正侵入判定ルールテーブル設定手段により、ルールテーブルを設定する際の履歴をテーブル変更保存手段により履歴テーブルに保存する。不正侵入判定ルールテーブル変更手段により、ルールテーブルを変更する際の履歴をテーブル変更保存手段により履歴テーブルに保存する。ＩＰアドレステーブル設定手段により、ＩＰアドレステーブルを設定する際の履歴をテーブル変更保存手段により履歴テーブルに保存する。ＩＰアドレス不正侵入判定ルールテーブル変更手段により、ＩＰアドレスルールテーブルを変更する際の履歴をテーブル変更保存手段により履歴テーブルに保存する。

【０１４４】この他の動作は、実施の形態１と同様である。

【０１４５】従って、ユーザによる設定変更および当侵入検知システムによる設定変更を後で確認することが可能となり管理負荷の低減と利便性が向上する。

【０１４６】実施の形態８．図１３は、実施の形態８における侵入検知システムを示す図である。本実施の形態における侵入検知システムは、前述の侵入検知システムの構成に加えて、通信手段７より得られるパケット６を保存しておくパケット保存手段６７と、パケット保存手段６７に保存されているパケット６を再生するパケット再生手段６８と、パケット再生手段６８にパケット６の再生を指示するパケット再生指示手段６９を備えている。尚、ここで再生するとは、保存されているパケットを通信手段によりネットワークへ送出することである。

【０１４７】動作について説明する。本実施の形態では、パケット保存手段６７により、通信手段７より得られるパケット６を保存し、パケット再生手段６８により、パケット保存手段６７に保存されているパケット６を再生する。ユーザーは、パケット再生指示手段６９により、パケット再生手段６８にパケット６の再生を指示する。

【０１４８】この他の動作は、実施の形態１と同様である。

【０１４９】従って、ユーザーの指定した時に、それまで保存しておいたパケット６の情報をもとに設定更新を実行させることができるので、企業等においては、ネットワーク５の混雑する昼間はパケット６を保存しておき、適当な時に設定更新作業を実施させることが可能である。

【０１５０】実施の形態９．図１４は、実施の形態９における侵入検知システムを示す図である。本実施の形態における侵入検知システムは、実施の形態８の侵入検知システムの構成に加えて、現在の日時を取得する日時取得手段７０と、パケット再生指示を出す日時を記述した再生スケジュール７１と、現在の日時と再生スケジュール７１を比較して指定された日時にパケット再生指示を出す指定日時パケット再生指示手段７２を備えている。

【０１５１】動作について説明する。本実施の形態では、指定日時パケット再生指示手段７２が、日時取得手段７０により現在の日時を取得し、再生スケジュール７１に記述されたパケット再生指示を出す日時と比較して、指定された日時にパケット再生指示をパケット再生手段６８に出す。

【０１５２】この他の動作は、実施の形態８と同様である。

【０１５３】従って、深夜等の利用者の少ない時間帯に設定更新作業を自動で実施させることが可能である。また、定期的に設定更新作業を実施させることも可能である。

【０１５４】実施の形態１０．図１５は、実施の形態１０における侵入検知システムを示す図である。本実施の形態における侵入検知システムは、実施の形態８の侵入検知システムの構成に加えて、システムの負荷状況を取得する負荷取得手段７３と、パケット再生指示を出すことのできる負荷情報を記述した再生可能負荷情報７４と、現在の負荷情報と再生可能負荷情報とを比較して可能な負荷状況であればパケット再生指示を出す低負荷時パケット再生指示手段７５を備えている。

【０１５５】動作について説明する。低負荷時パケット再生指示手段７５が、負荷取得手段７３によりシステムの負荷状況を取得し、再生可能負荷情報７４に記述されたパケット再生指示を出すことのできる負荷情報と比較して、可能な負荷状況であればパケット再生指示をパケット再生手段６８に出す。

【０１５６】この他の動作は、実施の形態８と同様である。なお、負荷取得手段７３は一定時間プログラムをループでまわし、その実行回数をカウントするなどの方法により実現される。

【０１５７】従って、システムの負荷の軽い時間帯に設定更新作業を自動で実施させることが可能であり、侵入検知機能のスループットを下げることが防げる。

【０１５８】実施の形態１１．図１６は、実施の形態１１における侵入検知システムを示す図である。本実施の形態における侵入検知システムは、実施の形態８の侵入検知システムの構成に加えて、パケット保存手段６７からパケット６の流通量を取得するパケット流通量取得手段７６と、パケット再生指示を出すことのできるパケット流通量を記述した再生可能流通量情報７７と、現在のパケット流通量と再生可能流通量情報７７とを比較して可能な流通量であればパケット再生指示を出す低ネットワーク負荷時パケット再生指示手段７８を備えている。

【０１５９】動作について説明する。低ネットワーク負荷時パケット再生指示手段７８が、パケット流通量取得手段７６によりパケット６の流通量を取得し、再生可能流通量情報７７に記述されたパケット再生指示を出すことのできるパケット流通量と比較して、可能な流通量であればパケット再生指示をパケット再生手段６８に出す。

【０１６０】この他の動作は、実施の形態８と同様である。

【０１６１】従って、ネットワークの負荷の軽い時間帯に設定更新作業を自動で実施させることが可能であり、ネットワークに繋がれた他の機器への影響を減らすことが可能である。

【０１６２】尚、上記の説明では、ネットワークにＷＷＷサーバやＭＡＩＬサーバがある場合について述べたが、その他のサーバに利用することも出来る。

【０１６３】

【発明の効果】本発明においては、自動的に更新されたＩＰアドレステーブル１０と不正侵入判定ルールテーブル１５を用いて侵入検知が実行されることとなる。

【０１６４】また、この発明は、ＩＰアドレステーブル１０にＩＰアドレス９が重複して設定されることがないので、ＩＰアドレステーブル１０が最適な状態に保たれる。

【０１６５】また、この発明は、不正侵入判定ルールテーブル１５にマシン名８とルール名１４のペアであるルールリストが重複して設定されることがないので、不正侵入判定ルールテーブル１５が最適な状態に保たれる。

【０１６６】また、この発明は、再検出の指定のみで自動的に更新されたＩＰアドレステーブル１０と不正侵入判定ルールテーブル１５を用いて侵入検知が実行されることとなる。

【０１６７】また、この発明は、何らかの異常が発生または設定の更新が必要と考えられる場合に、迅速に対応することが可能となる。

【０１６８】また、この発明は、管理者と当侵入検知システム以外の者により、設定情報が改ざんされることを防止できる。

【０１６９】また、この発明は、ユーザによる設定変更および当侵入検知システムによる設定変更を後で確認す

ることが可能となり管理負荷の低減と利便性が向上する。

【０１７０】また、この発明は、ユーザーの指定した時に、それまで保存しておいたパケット６の情報をもとに設定更新を実行させることができるので、企業等においては、ネットワーク５の混雑する昼間はパケット６を保存しておき、適当な時に設定更新作業を実施させることが可能である。

【０１７１】また、この発明は、深夜等の利用者の少ない時間帯に設定更新作業を自動で実施させることが可能である。また、定期的に設定更新作業を実施させることも可能である。

【０１７２】また、この発明は、システムの負荷の軽い時間帯に設定更新作業を自動で実施させることが可能であり、侵入検知機能のスループットを下げることが防げる。

【０１７３】また、この発明は、ネットワークの負荷の軽い時間帯に設定更新作業を自動で実施させることが可能であり、ネットワークに繋がれた他の機器への影響を減らすことが可能である。

【図面の簡単な説明】

【図１】　実施の形態１における侵入検知システムを示す図である。

【図２】　ＩＰアドレステーブルの構成を示す図である。

【図３】　ルールテーブルの構成を示す図である。

【図４】　検出ルールリストの構成を示す図である。

【図５】　WWWサーバ用検出ルールの処理の流れを示す図である。

【図６】　実施の形態２における侵入検知システムを示す図である。

【図７】　実施の形態３における侵入検知システムを示す図である。

【図８】　実施の形態４における侵入検知システムを示す図である。

【図９】　実施の形態５における侵入検知システムを示す図である。

【図１０】　実施の形態６における侵入検知システムを示す図である。

【図１１】　実施の形態７における侵入検知システムを示す図である。

【図１２】　この発明における履歴テーブルの構成の一例を示す図である。

【図１３】　実施の形態８における侵入検知システムを示す図である。

【図１４】　実施の形態９における侵入検知システムを示す図である。

【図１５】　実施の形態１０における侵入検知システムを示す図である。

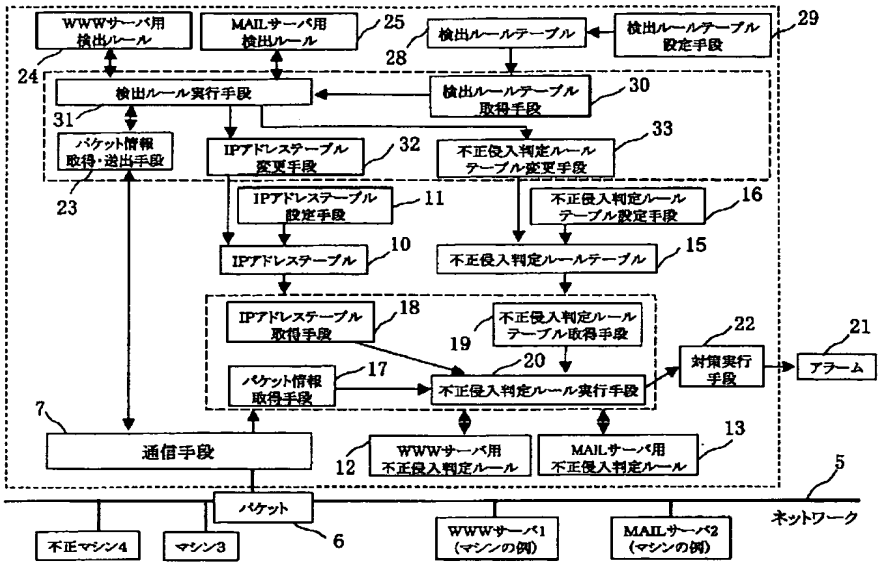
【図１６】　実施の形態１１における侵入検知システムを示す図である。

【図１７】　従来の侵入検知システムを示す図である。

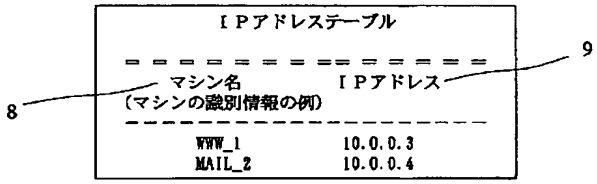
【符号の説明】

１　WWWサーバ、２　ＭＡＩＬサーバ、３　正常マシン、４　不正マシン、５　ネットワーク、６　パケット、７　通信手段、８　マシン名、９　ＩＰアドレス、１０　ＩＰアドレステーブル、１１　ＩＰアドレステーブル設定手段、１２　WWWサーバ用不正侵入判定ルール、１３　ＭＡＩＬサーバ用不正侵入判定ルール、１４　不正侵入判定ルール名、１５　不正侵入判定ルールテーブル、１６　不正侵入判定ルールテーブル設定手段、１７　パケット情報取得手段、１８ＩＰアドレステーブル取得手段、１９　不正侵入判定ルールテーブル取得手段、２０　不正侵入判定ルール実行手段、２１　アラーム、２２　対策実行手段、２３　パケット情報取得・送出手段、２４　WWWサーバ用検出ルール、２５ＭＡＩＬサーバ用検出ルール、２６　種類、２７　検出ルール、２８　検出ルールテーブル、２９　検出ルールテーブル設定手段、３０　検出ルールテーブル取得手段、３１　検出ルール実行手段、３２　ＩＰアドレステーブル変更手段、３３　不正侵入判定ルールテーブル変更手段、４３　ＩＰアドレス設定済検査手段、４４　不正侵入判定ルール設定済検査手段、４５　ＩＰアドレステーブル再取得手段、４６　不正侵入判定ルールテーブル再取得手段、４７　検出ルール再実行手段、４８　再検出指定手段、４９　アラーム検出手段、５１　設定時パスワード入力手段、５２　起動時パスワード入力手段、５３　実行時パスワード保存手段、５４　暗号済検出ルールテーブル、５５　検出ルールテーブル暗号設定手段、５６　検出ルールテーブル復号取得手段、５７　暗号済ＩＰアドレステーブル，５８　ＩＰアドレステーブル暗号設定手段、５９　ＩＰアドレステーブル復号取得手段、６０　ＩＰアドレステーブル暗号変更手段、６１　暗号済不正侵入判定ルールテーブル、６２　不正侵入判定ルールテーブル暗号設定手段、６３不正侵入判定ルールテーブル復号取得手段、６４　不正侵入判定ルールテーブル暗号変更手段、６５　履歴テーブル、６６　テーブル変更保存手段、６７　パケット保存手段、６８　パケット再生手段、６９　パケット再生指示手段、７０日時取得手段、７１　再生スケジュール、７２　指定日時パケット再生指示手段、７３　負荷取得手段、７４　再生可能負荷情報、７５　低負荷時パケット再生指示手段、７６　パケット流通量取得手段、７７　再生可能流通量情報、７８低ネットワーク負荷時パケット再生指示手段。

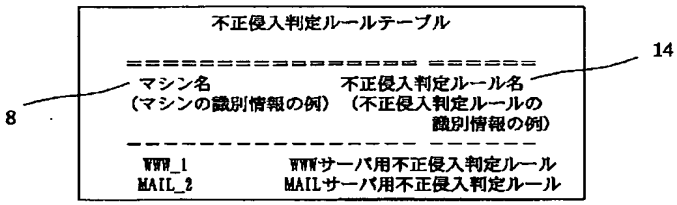
【図１】



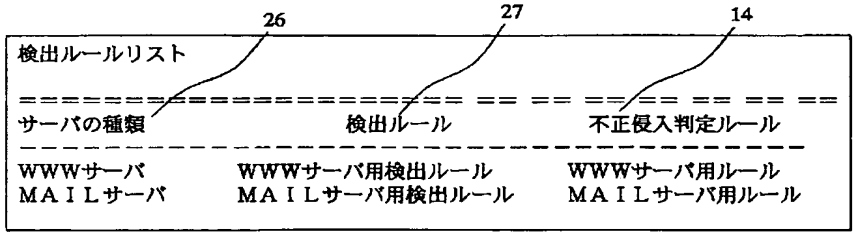
【図２】



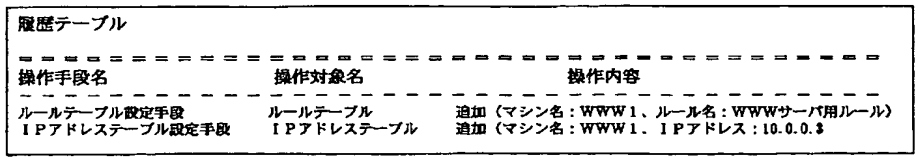
【図３】



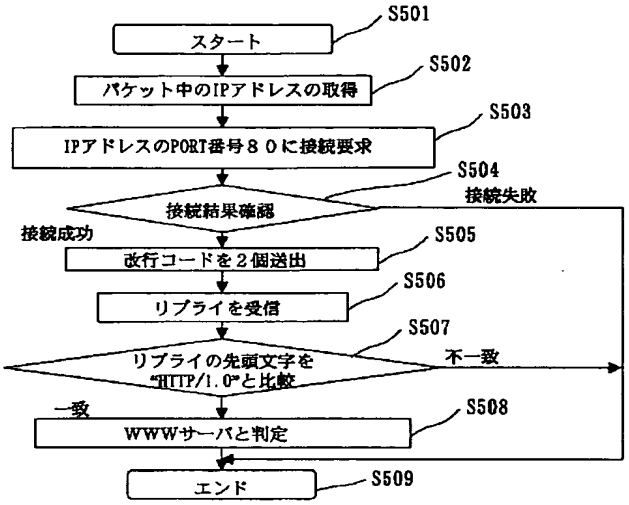
【図４】



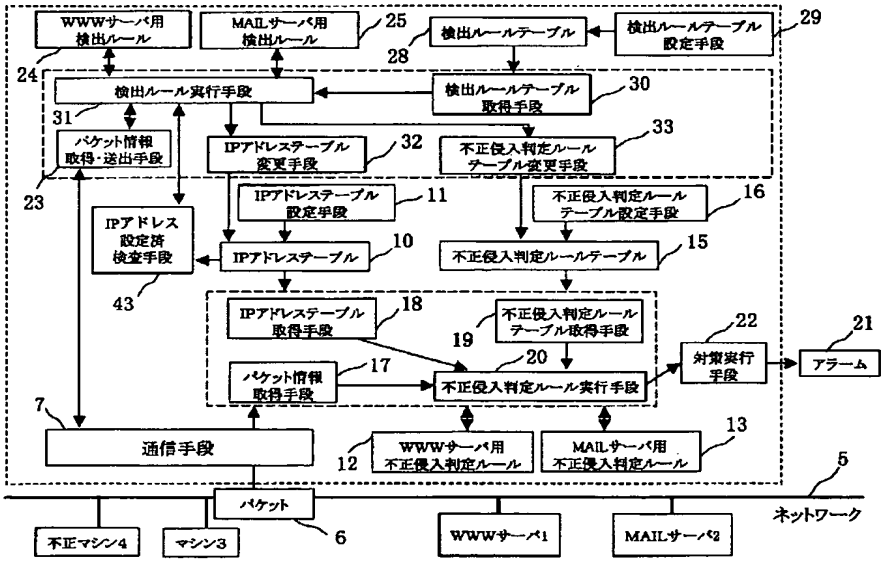
【図１２】



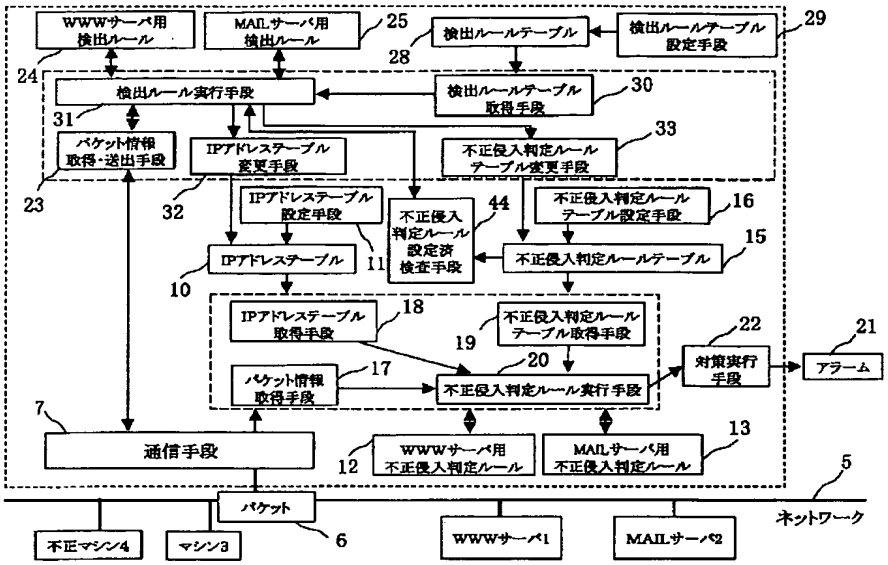
【図５】


S501
スタート
S502
パケット中のIPアドレスの取得
S503
IPアドレスのPORT番号８０に接続要求
S504
接続結果確認
接続失敗
接続成功
S505
改行コードを２個送出
S506
リプライを受信
S507
リプライの先頭文字を
"HTTP/1.0"と比較
不一致
一致
S508
WWWサーバと判定
エンド
S509

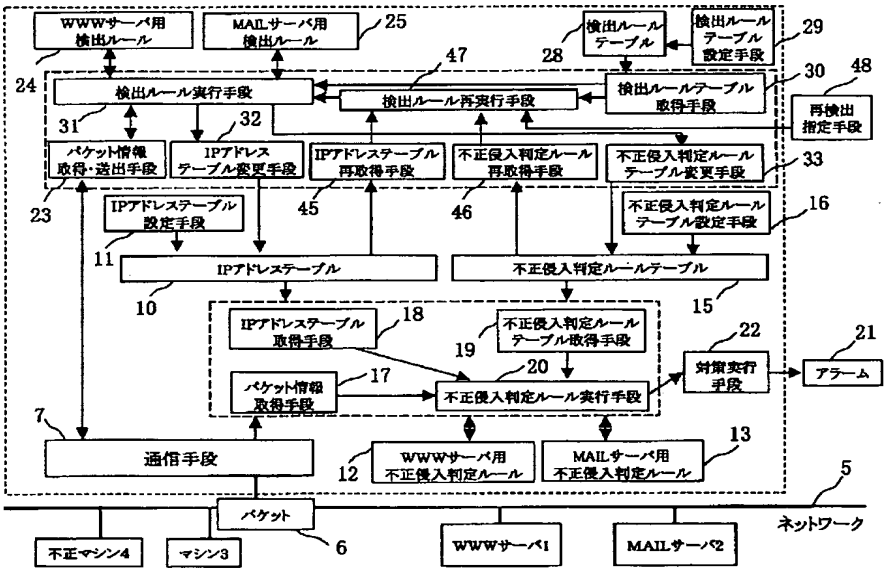
【図６】


WWWサーバ用
検出ルール
MAILサーバ用
検出ルール
25
検出ルールテーブル
検出ルールテーブル
設定手段
29
28
24
検出ルール実行手段
検出ルールテーブル
取得手段
30
31
パケット情報
取得・送出手段
IPアドレステーブル
変更手段
32
不正侵入判定ルール
テーブル変更手段
33
23
IPアドレステーブル
設定手段
11
不正侵入判定ルール
テーブル設定手段
16
IPアドレス
設定済
検査手段
IPアドレステーブル
10
不正侵入判定ルールテーブル
15
43
IPアドレステーブル
取得手段
18
不正侵入判定ルール
テーブル取得手段
19
22
21
パケット情報
取得手段
17
20
不正侵入判定ルール実行手段
対策実行
手段
アラーム
7
通信手段
12
WWWサーバ用
不正侵入判定ルール
MAILサーバ用
不正侵入判定ルール
13
5
パケット
6
ネットワーク
不正マシン4
マシン3
WWWサーバ1
MAILサーバ2

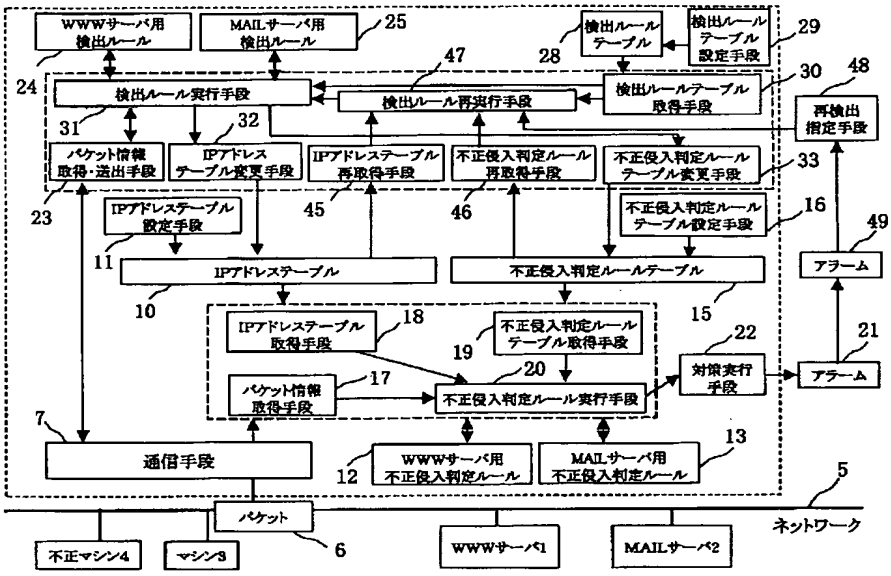
【図７】


WWWサーバ用検出ルール
MAILサーバ用検出ルール
検出ルールテーブル
検出ルールテーブル設定手段
検出ルール実行手段
検出ルールテーブル取得手段
パケット情報取得・送出手段
IPアドレステーブル変更手段
不正侵入判定ルールテーブル変更手段
IPアドレステーブル設定手段
不正侵入判定ルール設定済検査手段
不正侵入判定ルールテーブル設定手段
IPアドレステーブル
不正侵入判定ルールテーブル
IPアドレステーブル取得手段
不正侵入判定ルールテーブル取得手段
パケット情報取得手段
不正侵入判定ルール実行手段
対策実行手段
アラーム
通信手段
WWWサーバ用不正侵入判定ルール
MAILサーバ用不正侵入判定ルール
パケット
ネットワーク
不正マシン4
マシン3
WWWサーバ1
MAILサーバ2

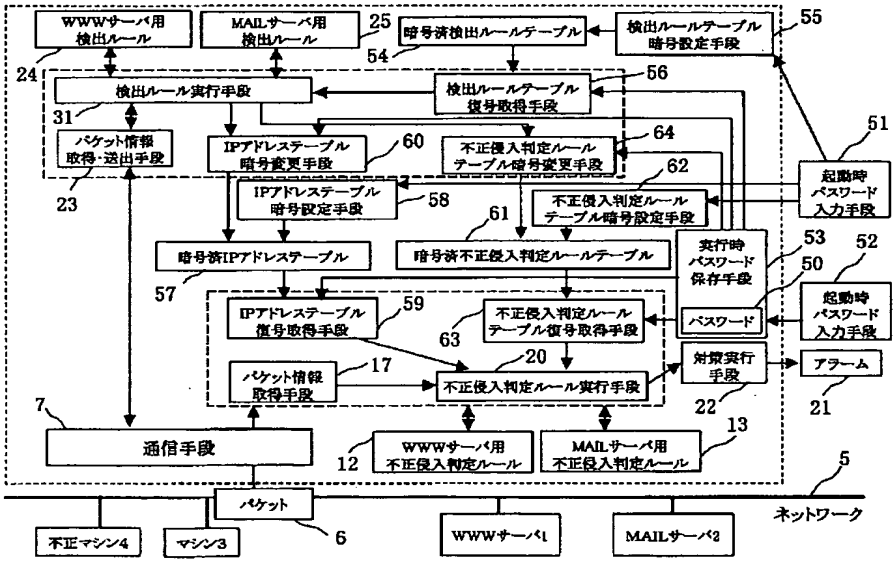
【図８】


WWWサーバ用検出ルール
MAILサーバ用検出ルール
検出ルールテーブル
検出ルールテーブル設定手段
検出ルール実行手段
検出ルール再実行手段
検出ルールテーブル取得手段
再検出指定手段
パケット情報取得・送出手段
IPアドレステーブル変更手段
IPアドレステーブル再取得手段
不正侵入判定ルール再取得手段
不正侵入判定ルールテーブル変更手段
IPアドレステーブル設定手段
不正侵入判定ルールテーブル設定手段
IPアドレステーブル
不正侵入判定ルールテーブル
IPアドレステーブル取得手段
不正侵入判定ルールテーブル取得手段
パケット情報取得手段
不正侵入判定ルール実行手段
対策実行手段
アラーム
通信手段
WWWサーバ用不正侵入判定ルール
MAILサーバ用不正侵入判定ルール
パケット
ネットワーク
不正マシン4
マシン3
WWWサーバ1
MAILサーバ2

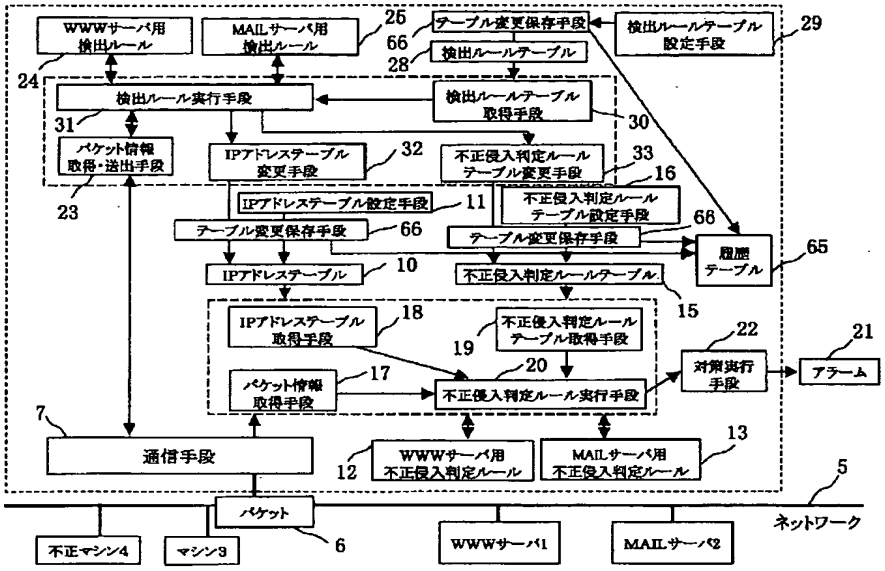
【図９】


WWWサーバ用検出ルール
MAILサーバ用検出ルール
25
検出ルールテーブル
28
検出ルールテーブル設定手段
29
24
検出ルール実行手段
47
検出ルール再実行手段
検出ルールテーブル取得手段
30
48
再検出指定手段
31
32
パケット情報取得・送出手段
IPアドレステーブル変更手段
IPアドレステーブル再取得手段
不正侵入判定ルール再取得手段
不正侵入判定ルールテーブル変更手段
33
23
45
46
IPアドレステーブル設定手段
不正侵入判定ルールテーブル設定手段
16
49
11
IPアドレステーブル
不正侵入判定ルールテーブル
アラーム
10
15
IPアドレステーブル取得手段
18
不正侵入判定ルールテーブル取得手段
19
22
21
パケット情報取得手段
17
20
不正侵入判定ルール実行手段
対策実行手段
アラーム
7
通信手段
12
WWWサーバ用不正侵入判定ルール
MAILサーバ用不正侵入判定ルール
13
5
ネットワーク
パケット
6
不正マシン4
マシン3
WWWサーバ1
MAILサーバ2

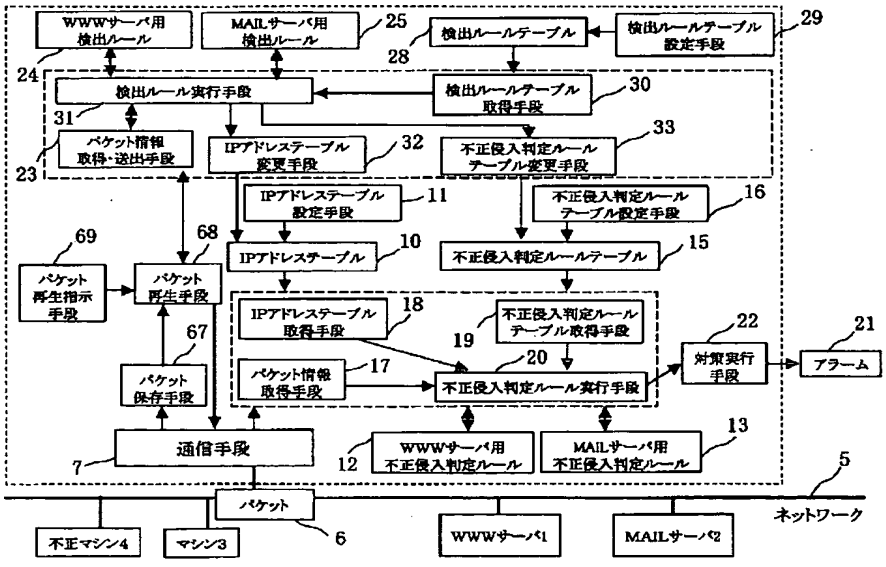
【図１０】


WWWサーバ用検出ルール
MAILサーバ用検出ルール
25
暗号済検出ルールテーブル
54
検出ルールテーブル暗号設定手段
55
24
検出ルール実行手段
検出ルールテーブル復号取得手段
56
31
パケット情報取得・送出手段
IPアドレステーブル暗号変更手段
60
不正侵入判定ルールテーブル暗号変更手段
64
51
23
IPアドレステーブル暗号設定手段
58
62
不正侵入判定ルールテーブル暗号設定手段
起動時パスワード入力手段
61
暗号済IPアドレステーブル
暗号済不正侵入判定ルールテーブル
実行時パスワード保存手段
53
52
57
50
IPアドレステーブル復号取得手段
59
不正侵入判定ルールテーブル復号取得手段
パスワード
起動時パスワード入力手段
63
パケット情報取得手段
17
20
不正侵入判定ルール実行手段
対策実行手段
アラーム
22
21
7
通信手段
12
WWWサーバ用不正侵入判定ルール
MAILサーバ用不正侵入判定ルール
13
5
ネットワーク
パケット
6
不正マシン4
マシン3
WWWサーバ1
MAILサーバ2

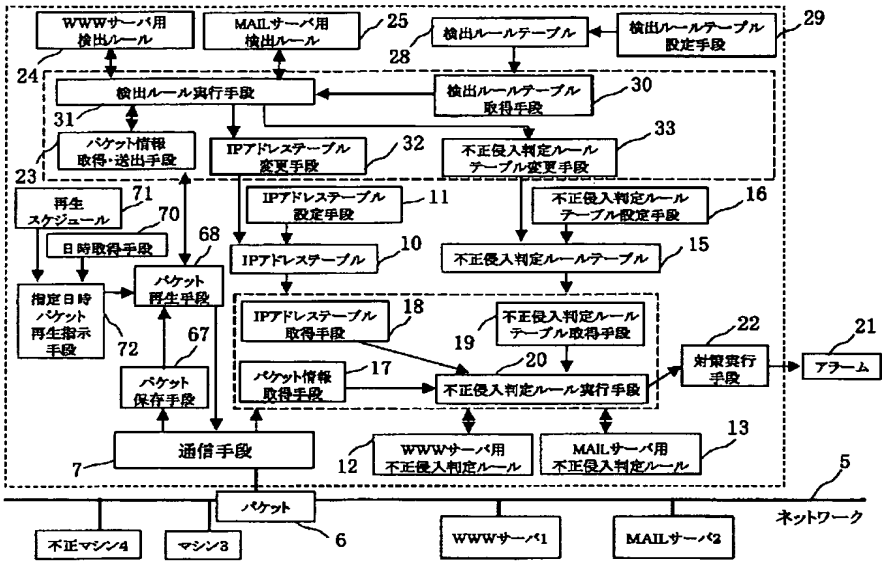
【図１１】


WWWサーバ用検出ルール
MAILサーバ用検出ルール
25
テーブル変更保存手段
検出ルールテーブル設定手段
29
66
検出ルールテーブル
28
24
検出ルール実行手段
検出ルールテーブル取得手段
30
31
パケット情報取得・送出手段
IPアドレステーブル変更手段
32
不正侵入判定ルールテーブル変更手段
33
16
23
IPアドレステーブル設定手段
11
不正侵入判定ルールテーブル設定手段
66
テーブル変更保存手段
66
テーブル変更保存手段
履歴テーブル
65
IPアドレステーブル
10
不正侵入判定ルールテーブル
15
IPアドレステーブル取得手段
18
不正侵入判定ルールテーブル取得手段
19
22
21
対策実行手段
アラーム
パケット情報取得手段
17
20
不正侵入判定ルール実行手段
7
通信手段
12
WWWサーバ用不正侵入判定ルール
MAILサーバ用不正侵入判定ルール
13
5
パケット
6
ネットワーク
不正マシン4
マシン3
WWWサーバ1
MAILサーバ2

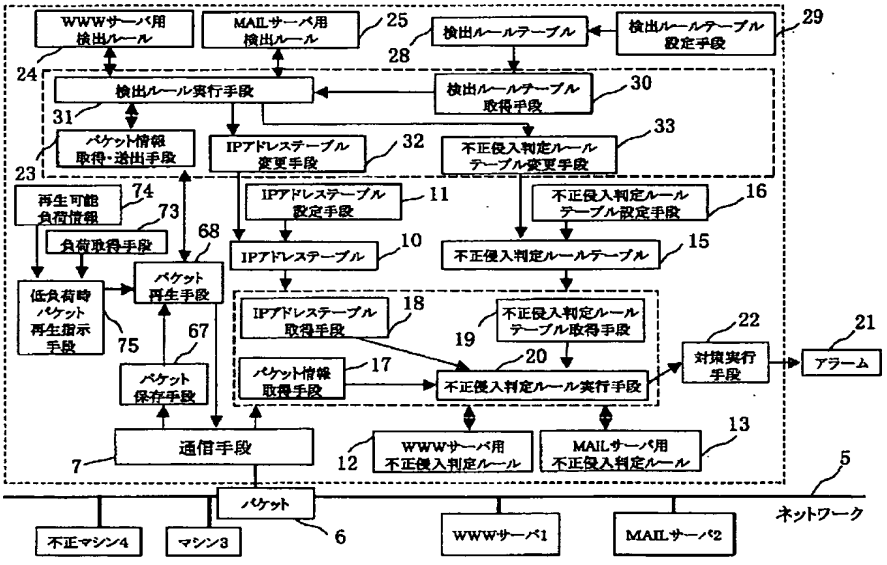
【図１３】


WWWサーバ用検出ルール
MAILサーバ用検出ルール
25
検出ルールテーブル
検出ルールテーブル設定手段
29
28
24
検出ルール実行手段
検出ルールテーブル取得手段
30
31
パケット情報取得・送出手段
IPアドレステーブル変更手段
32
不正侵入判定ルールテーブル変更手段
33
23
IPアドレステーブル設定手段
11
不正侵入判定ルールテーブル設定手段
16
69
68
パケット再生指示手段
パケット再生手段
IPアドレステーブル
10
不正侵入判定ルールテーブル
15
IPアドレステーブル取得手段
18
不正侵入判定ルールテーブル取得手段
19
22
21
67
パケット保存手段
パケット情報取得手段
17
20
対策実行手段
アラーム
不正侵入判定ルール実行手段
通信手段
7
12
WWWサーバ用不正侵入判定ルール
MAILサーバ用不正侵入判定ルール
13
5
パケット
6
ネットワーク
不正マシン4
マシン3
WWWサーバ1
MAILサーバ2

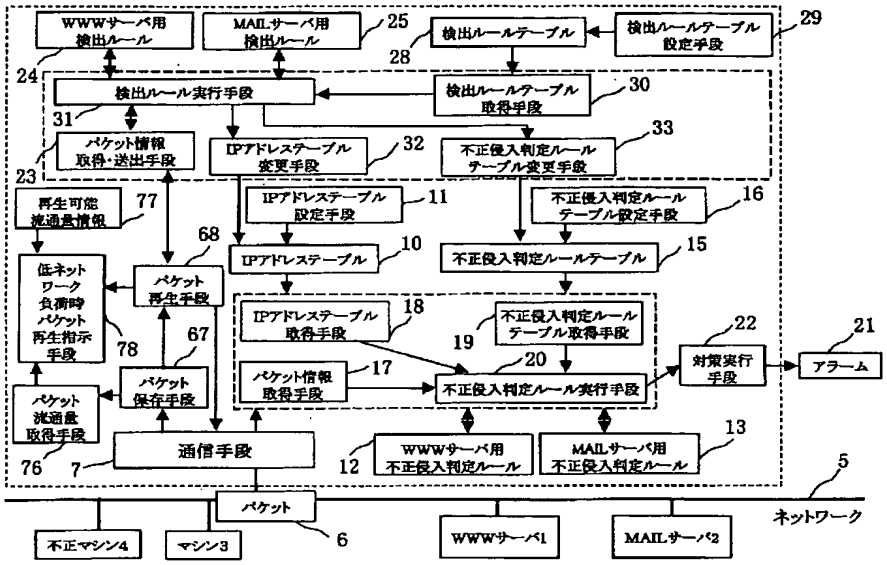
【図１４】


WWWサーバ用検出ルール
MAILサーバ用検出ルール
25
検出ルールテーブル
検出ルールテーブル設定手段
29
28
24
検出ルール実行手段
検出ルールテーブル取得手段
30
31
パケット情報取得・送出手段
IPアドレステーブル変更手段
32
不正侵入判定ルールテーブル変更手段
33
23
再生スケジュール
71
IPアドレステーブル設定手段
11
不正侵入判定ルールテーブル設定手段
16
70
日時取得手段
68
IPアドレステーブル
10
不正侵入判定ルールテーブル
15
パケット再生手段
指定日時パケット再生指示手段
72
IPアドレステーブル取得手段
18
不正侵入判定ルールテーブル取得手段
19
22
21
67
パケット情報取得手段
17
20
不正侵入判定ルール実行手段
対策実行手段
アラーム
パケット保存手段
通信手段
7
12
WWWサーバ用不正侵入判定ルール
MAILサーバ用不正侵入判定ルール
13
5
パケット
6
ネットワーク
不正マシン4
マシン3
WWWサーバ1
MAILサーバ2

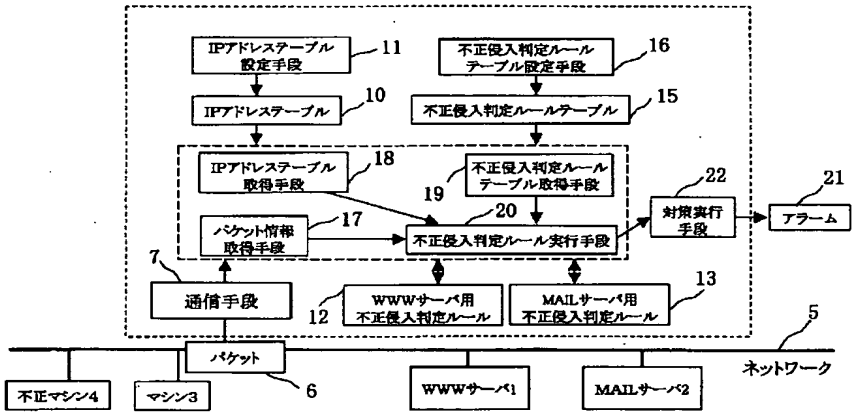
【図１５】


WWWサーバ用検出ルール
MAILサーバ用検出ルール
25
検出ルールテーブル
検出ルールテーブル設定手段
29
28
24
検出ルール実行手段
検出ルールテーブル取得手段
30
31
パケット情報取得・送出手段
IPアドレステーブル変更手段
32
不正侵入判定ルールテーブル変更手段
33
23
再生可能負荷情報
74
IPアドレステーブル設定手段
11
不正侵入判定ルールテーブル設定手段
16
73
負荷取得手段
68
IPアドレステーブル
10
不正侵入判定ルールテーブル
15
パケット再生手段
低負荷時パケット再生指示手段
75
IPアドレステーブル取得手段
18
不正侵入判定ルールテーブル取得手段
19
22
21
67
パケット情報取得手段
17
20
不正侵入判定ルール実行手段
対策実行手段
アラーム
パケット保存手段
通信手段
7
12
WWWサーバ用不正侵入判定ルール
MAILサーバ用不正侵入判定ルール
13
5
パケット
6
ネットワーク
不正マシン4
マシン3
WWWサーバ1
MAILサーバ2

【図１６】


WWWサーバ用検出ルール
MAILサーバ用検出ルール
検出ルールテーブル
検出ルールテーブル設定手段
検出ルール実行手段
検出ルールテーブル取得手段
パケット情報取得・送出手段
IPアドレステーブル変更手段
不正侵入判定ルールテーブル変更手段
再生可能流通量情報
IPアドレステーブル設定手段
不正侵入判定ルールテーブル設定手段
IPアドレステーブル
不正侵入判定ルールテーブル
低ネットワーク負荷時パケット再生指示手段
パケット再生手段
IPアドレステーブル取得手段
不正侵入判定ルールテーブル取得手段
パケット情報取得手段
不正侵入判定ルール実行手段
対策実行手段
アラーム
パケット流通量取得手段
パケット保存手段
通信手段
WWWサーバ用不正侵入判定ルール
MAILサーバ用不正侵入判定ルール
パケット
ネットワーク
不正マシン4
マシン3
WWWサーバ1
MAILサーバ2
24
25
28
29
31
30
23
32
33
77
11
16
68
10
15
18
19
22
21
78
67
17
20
76
7
12
13
5
6

【図１７】


IPアドレステーブル設定手段
不正侵入判定ルールテーブル設定手段
IPアドレステーブル
不正侵入判定ルールテーブル
IPアドレステーブル取得手段
不正侵入判定ルールテーブル取得手段
パケット情報取得手段
不正侵入判定ルール実行手段
対策実行手段
アラーム
通信手段
WWWサーバ用不正侵入判定ルール
MAILサーバ用不正侵入判定ルール
パケット
ネットワーク
不正マシン4
マシン3
WWWサーバ1
MAILサーバ2
11
16
10
15
18
19
22
21
17
20
7
12
13
5
6